INFORMATION AND CONTROL 4, 324–331 (1961)

Multiple Burst Error Correction*

JEREMY J. STONE

Mathematical Sciences Department, Stanford Research Institute, Menlo Park, California

Two results on the correction of multiple bursts of errors are presented. In Section II, a theorem is given which increases the feasibility of correcting such errors in codes over $GF(2)$ by constructing cyclic codes of a given weight. In Section III, a method is given for constructing quasi-cylic codes over $GF(p^k)$ which will correct multiple bursts of errors.

I. INTRODUCTION

A. SUMMARY

In the literature on error correction codes there has been a good deal of attention given to the correction of a (single) burst of errors; see for example (Peterson, 1961, Chap. 10). The problem of treating multiple bursts of errors is still more complicated and has received correspondingly less attention. The two theorems presented here are attempts to reduce the difficulties of the multiple burst correction case to the construction of certain types of codes of a given weight, i.e., to aspects of multiple (single) *error* correction. The first theorem shows that *cyclic* codes of a given weight over $GF(2)$ are almost 50% more efficient than might be supposed in the correction of multiple bursts of errors. The construction of such codes has been well discussed, see e.g., (Bose-Chaudhuri, 1960a, 1960b, and Peterson, 1961). The second theorem indicates that m multiple bursts of width p or less might be handled by adapting certain very efficient quasicyclic codes of weight $2m + 1$ over $GF(p^k)$.

B. DEFINITIONS

Let $V_n(GF(p^k))$ be the n-dimensional vector space over the Galois Field with p^k elements. Certain elements $v = (a_0, a_1, \cdots, a_{n-1})$ of

* This work was done on a project sponsored by the Air Force Systems Command, Rome Air Development Center, Griffiss Air force Base, New York. I am indebted to the project leader, Dr. Bernard Elspas for stimulating conversations and especially for posing this problem of multiple burst error correction.

this vector space are to be conceived of as representing a message, and this message is to be transmitted over a channel by sending in order a_{n-1}, a_{n-2}, $\cdots$, a_0. The vectors representing messages will be called the code. The codes discussed here will be group codes, i.e., the vectors of the code will form a subgroup of $GF(p^k)$. Errors in transmission may occur. It is assumed however that some, possibly distorted, vector $v' = (a_0', a_1', \cdots, a_{n-1}')$ will be received and the distortion or error e is taken to be

$$e = v' - v = (a_0' - a_0, a_1' - a_1, \cdots, a_{n-1}' - a_{n-1}).$$

If a certain class P of errors is anticipated and a code specified, the question arises whether there exists a rule which correctly decodes the received vectors so long as it is correct to assume that a code vector was sent and that the error e involved is a member of P. If v_i' represents the form in which v_i is received after the addition of an error e_i, the desired rule will exist if and only if, whenever

$$\begin{gathered} v_1' = v_1 + e_1 = v_2 + e_2 = v_2' \\ e_i \text{ in } P, v_i \text{ in code } \quad i = 1, 2 \end{gathered} \tag{1}$$

we have

$$v_1 = v_2 . \tag{2}$$

For group codes an equivalent condition is: If $e_1 - e_2$ is in the code, and e_i is in P, then $e_1 = e_2$. We take as a

DEFINITION: A group code C corrects a class of errors P if and only if $e_1 - e_2$ in C and e_1, e_2 in P implies $e_1 = e_2$.

A burst error of width b is a vector whose components are zero outside of a set of b adjacent components the first and last of which are non-zero. (The last component a_{n-1} is understood to be adjacent to a_0.) In this paper P is taken to be the set of all vectors which can be formed from a sum of at most m burst errors of width b or less. If

$$v = (a_0, a_1, \cdots, a_{n-1})$$

is in $V_n(GF(p^k))$, let g_v be the polynomial over $GF(p^k)$ defined by $g_v(x) = \sum_{i=0}^{n-1} a_i x^i$. If there exists a polynomial g over $GF(p^k)$ such that

$$C = \{v : g \mid g_v\} \tag{3}$$

C is called a quasi-cyclic code. If in addition n is the period[1] of g, C is

[1] The period of an element θ in $GF(p^k)$ is the least integer n for which $\theta^n = 1$. The period of a polynomial f over $GF(p^k)$ is the least integer n for which f divides $x^n - 1$ over $GF(p^k)$.

called a cyclic code. (It is easy to check that, for such a code,

$$v = (a_0, a_1, \cdots, a_{n-1})$$

in C implies that the cyclic permutations of v, e.g., $(a_n, a_0, a_1, \cdots, a_{n-1})$, are in C.) These codes are clearly group codes.

If v is in $V_n(GF(p^k))$, let the weight of v denoted by $\omega(v)$ be the number of nonzero places in v. The weight of a code C is defined to be the minimum of the nonzero weights of members of C. The weight of a polynomial h over $GF(p^k)$, denoted $\omega(h)$, is the number of nonzero coefficients of h. $[x]$ denotes the greatest integer less than or equal to x. The redundancy of the quasi-cyclic code C is defined to be the degree of g.

II. CORRECTION OF MULTIPLE BURSTS WITH CYCLIC CODES OVER $GF(2)$ OF A GIVEN WEIGHT

If a cyclic code C has weight $2mt + 1$, it is easy to check that it will correct the class P consisting of up to m bursts of size t. The theorem below and a following comment show that C actually corrects m-multiple bursts of width larger than t. The increase is usually by a factor of almost 50%.

THEOREM 1. *If $C \subset V_n(GF(2))$ is a cyclic code of weight $2mt + 1$ and $n > 3mt$, then C corrects the class P of all sums of up to m bursts of width $b = t + [(t - 2)/2 + 3/(4m)]$ or less. For $m = 1$ this gives $b = t + [(2t - 1)/4]$ while for $m \geqq 2$, $b = t + [(t - 2)/2]$.*

PROOF: Since C is a cyclic code there exists a polynomial g over $GF(2)$ whose period is n and such that

$$C = \{v : g \mid g_v\}. \tag{4}$$

Assume that $e_1 - e_2$ is in C, and that e_1 and e_2 are in P. It must then be shown that $e_1 - e_2 = 0$. The assumption on n implies $n > 2mb$ and hence the vector $e_1 - e_2$ has at least one component which is zero. Since C is cyclic there is a cyclic permutation of $e_1 - e_2$ which is in C and which has zero in the last place. If this permutation is proved to be zero, $e_1 - e_2$ would be zero, so we may restrict ourselves to proving that $e_1 - e_2$ in C implies $e_1 = e_2$ for vectors $e_1 - e_2$ which are zero in the last place. Furthermore we may assume that

$$\omega(e_1) + \omega(e_2) \geqq 2mt + 1 \tag{5}$$

for if not

$$\omega(e_1 - e_2) \leqq \omega(e_1) + \omega(e_2) < 2mt + 1 \tag{6}$$

and since C has weight $2mt + 1$, $e_1 - e_2$ in C implies $e_1 - e_2 = 0$ immediately. Since e_j, $j = 1, 2$, are in P, we have

$$g_{e_j} = \sum_{i=1}^{m} x^{k_i} E_{ij} \tag{7}$$

where E_{ij} is a polynomial over $GF(2)$ with constant term and degree less than $t + s$, $s = [(t - 2)/2 + 3/(4m)]$ (for each j, the E_{ij} are taken to represent disjoint bursts). Using $1 + 1 = 0$, E_{ij} can be written in the form

$$E_{ij} = \sum_{a=0}^{t+s-1} x^a + \sum_{k=1}^{a_{ij}} x^{a_{ijk}} \qquad \begin{matrix} i = 1, 2, \cdots, m \\ j = 1, 2 \\ 0 \leqq a_{ijk} \leqq t + s - 1 \end{matrix} \tag{8}$$

where the a_{ijk} indicate the coefficients of E_{ij} which are zero, and a_{ij} indicates the total number of these coefficients. Evidently,

$$\omega(E_{ij}) = t + s - a_{ij} . \tag{9}$$

Since $\omega(g_{e_j}) = \omega(e_j)$ we can substitute (9) and (7) into (5) giving

$$\begin{aligned} \sum_{i=1}^{m} t + s - a_{i1} + \sum_{i=1}^{m} t + s - a_{i2} \\ = 2m(t + s) - \sum_{i,j} a_{ij} \geqq 2mt + 1 \end{aligned} \tag{10}$$

or

$$2ms - 1 \geqq \sum_{i,j} a_{ij} . \tag{11}$$

Notice now that in (8), $(1 + x)$ multiplied by the first sum gives $1 + x^{t+s}$, a polynomial of weight 2, while $(1 + x)$ times the second sum gives a polynomial of weight at most $2a_{ij}$. Hence

$$\omega((1 + x)E_{ij}) \leqq 2 + 2a_{ij} \tag{12}$$

and therefore

$$\begin{aligned} \omega((1 + x)g_{e_1 - e_2}) &\leqq \omega((1 + x)g_{e_1}) + \omega((1 + x)g_{e_2}) \\ &\leqq \sum_{i=1}^{m} \omega((1 + x)E_{i1}) + \sum_{i=1}^{m} \omega((1 + x)E_{i2}) \\ &\leqq \sum_{i,j} 2 + 2a_{ij} = 4m + 2\sum_{i,j} a_{ij} . \end{aligned} \tag{13}$$

Since we assumed earlier that $g_{e_1-e_2}$ had degree less than $n-1$,

$$(1+x)g_{e_1-e_2}$$

has degree $n-1$ at most and therefore there exists a vector η such that $g_\eta = (1+x)g_{e_1-e_2}$. According to (3), $C = \{v : g \mid g_v\}$ for some g and since divisors of $g_{e_1-e_2}$ will divide g_η, $e_1 - e_2$ in C implies η in C. We proceed to show that $\eta = 0$ which will imply $g_\eta = 0$, hence

$$(1+x)g_{e_1-e_2} = 0$$

or $e_1 = e_2$. From (13) and (11)

$$\omega(g_\eta) \leqq 4m + 2\sum_{i,j} a_{ij} \leqq 4m + 4ms - 2. \tag{14}$$

Substituting $s = [(t-2)/2] + 3/(4m)$ into (14) and noting that $[(t-2)/2 + 3/(4m)]$ is not an integer gives

$$\omega(g_\eta) \leqq 4m + 4m\left[\frac{2mt - 4m + 3}{4m}\right] \tag{15}$$

$$-2 < 4m + 2mt - 4m + 3 - 2 = 2mt + 1.$$

Since η is in C which has weight $2mt+1$, $\eta = 0$ which as noted above gives $e_1 = e_2$. This completes the proof except to remark that for $m \geqq 2$, $[(t-2)/2 + 3/(4m)] = (t-2)/2$.

As an example, consider a code of weight 25 and block length greater than 36. Setting $2mt + 1 = 25$ or $mt = 12$ we construct the following table, Table I, which shows that for the correction of single, double or triple bursts the theorem would be useful (for 4, 6, or 12 bursts it gives no non-trivial information).

We note that the only use of the assumption $n > 3mt$ was to ensure $n > 2mb$ for the burst width b to be corrected. In general, for a cyclic

TABLE I

$n > 36$

m	t	b	mb
1	12	17	17
2	6	8	16
3	4	5	15
4	3	3	12
6	2	2	12
12	1	1	12

code C of weight $2mt + 1$, if

$$b = \min\left(\left[\frac{n-1}{2m}\right], t + \left[\frac{t-2}{2} + \frac{3}{4m}\right]\right)$$

essentially the same proof as above will show that C corrects m-multiple bursts of width b.

If the errors which are anticipated are sums of multiple bursts and occasional single errors,[2] a theorem similar to Theorem 1 can be proved. For example, if P consists of sums of up to m bursts of width b and at most u single errors, a code of weight $2(mt + u) + 1$ where

$$t \geqq \tfrac{2}{3}b + 1 + [(2u - 3)/6m]$$

will correct P [with $n > 2(mt + u)$]. Since obviously a code of weight $2(mb + u) + 1$ would correct P the saving depends on having

$$1 + [(2u - 3)/6m]$$

somewhat less than $b/3$. This gives some indication of the fact that, although other similar theorems can be constructed which allow some double errors etc., as well as single errors to be handled along with the larger multiple bursts, the gain in efficiency shown by these theorems will deteriorate (unless b and m are kept large).

III. CORRECTION OF MULTIPLE BURSTS OF ERRORS THROUGH THE USE OF DIFFERENTIATION OVER FIELDS $GF(p^k)$

THEOREM 2.[3] *Let f be a polynomial over $GF(p^k)$ with degree d which generates a quasi-cyclic code in $V_n(GF(p^k))$ of weight at least $2m + 1$ and assume $pd < n$. Then the quasi-cyclic code in $V_n(GF(p^k))$ which is generated by f^p corrects m-multiple bursts of width less than or equal to p.*

PROOF: It must be shown that if e_j, $j = 1, 2$, are errors of the kind in question, that $e_1 - e_2$ in C implies $e_1 = e_2$. Let

$$g_{e_1-e_2}(x) = \sum_{j=1}^{2} \sum_{i=1}^{m} x^{k_{ij}} E_{ij}(x) \qquad 0 \leqq k_{ij} < n \quad (16)$$

[2] The desirability of correcting such errors was suggested by the project monitor, Dr. Jack K. Wolf.

[3] *Note added in proof:* A letter published in the August 1961 *Proc. IRE* by Francis Corr, entitled, "Multiple Burst Detection," discusses cyclic codes generated by $f(x^b)$ where b is the size of bursts which one desires to correct or detect. If k is taken to be one, the above theorem establishes shortened versions of a special case of these codes for which $f(x^b) = f^b(x)$.

where E_{ij} is a polynomial over $GF(p^k)$ with constant term and degree less than p. If $e_1 - e_2$ were in C then there would exist a polynomial h over $GF(p^k)$ such that

$$hf^p = g_{e_1-e_2}. \tag{17}$$

Since $pf^{p-1} = 0$, this implies by taking derivatives that

$$f^p \mid g^{(q)}_{e_1-e_2} \qquad q = 0, 1, 2, \cdots, p-1 \tag{18}$$

where (q) denotes kth order differentiation over $GF(p^k)$. Let q_o, $0 \leqq q_0 \leqq p$, be the first q for which $g^{(q)}_{e_1-e_2} = 0$. If $q_o \neq 0$ then by (18),

$$f \mid g^{(q_o-1)}_{e_1-e_2}$$

and

$$g^{(q_o-1)}_{e_1-e_2} \neq 0.$$

However $g^{(q_o-1)}_{e_1-e_2}$ is evidently a polynomial in x^p and consideration of (16) indicates that it can have no more than $2m$ nonzero terms. Since f does not divide such polynomials, we must have $q_o = 0$. Hence

$$g_{e_1-e_2} = 0 \qquad \text{or} \qquad e_1 = e_2$$

which completes the proof.

To use Theorem 2 efficiently, one must take considerable care to find an f of the kind desired with as small a degree d as one can, since the redundancy of the code is pd. The saving presented by reducing the degree of f might make computational methods worthwhile in its construction. However, if f is constructed by the Bose-Chaudhuri method (so that it has the roots $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2m}$) it will generally be true that the redundancy resulting from Theorem 2 is sufficient to construct a Bose-Chaudhuri code (associated with a polynomial g with roots $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2pm}$) which will correct *all* errors of weight pm or less. Thus if f cannot be constructed in a more efficient way the only advantage of Theorem 2 is that the construction of f^p which only involves raising f to the pth power (over a field of characteristic p) is much simpler than the more extended operations with roots involved in constructing g. An example of this is given below.

Example

$$f(x) = (x^7 + x^3 + 1)(x^7 + x^3 + x^2 + x + 1)$$
$$(x^7 + x^4 + x^3 + x^2 + 1)$$

has period $n = 127$ and is a Bose-Chaudhuri code over $GF(2)$ with roots $\alpha, \alpha^2, \cdots, \alpha^6$ generating a code of weight at least 7. This gives $m = 3$. Since $p = 2$, by Theorem 2

$$f^2(x) = (x^{14} + x^6 + 1)(x^{14} + x^6 + x^4 + x^2 + 1)$$
$$(x^{14} + x^8 + x^6 + x^4 + 1)$$

generates a quasi-cyclic code with $n = 127$ which corrects all triple bursts of width at most $p = 2$. The corresponding Bose-Chaudhuri code which corrects all errors of weight $3 \cdot 2 = 6$ or less is generated by

$$g(x) = (x^7 + x^3 + 1)(x^7 + x^3 + x^2 + x + 1)$$
$$(x^7 + x^4 + x^3 + x^2 + 1)(x^7 + x^6 + x^5 + x^4 + x^2 + x + 1)$$
$$(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^7 + x^6 + x^4 + x^2 + 1)$$

f^2 and g correspond to the same rate of transmission of information.

RECEIVED: June 26, 1961.

REFERENCES

BOSE, R. C., AND RAY-CHAUDHURI, D. K. (1960a). On a class of error correcting binary group codes, *Information and Control* 3, 68–79.

BOSE, R. C., AND RAY-CHAUDHURI, D. K. (1960b). Further results on error correcting binary group codes, *Information and Control* 3, 279–290.

FIRE, P. (1959). A class of multiple-error-correcting binary codes for non-independent errors, *Sylvania Rept. RSL-E-2*, Sylvania Reconnaissance Systems Laboratory, Mountain View, California.

PETERSON, W. W. (1961). "Error Correcting Codes." Mass. Inst. Technol. Press and Wiley, New York.